Sqlandsecurity

Technology, Information Technology

SQL and Security Answers to the assignment SQL Injection is a form of database attack where the attacker attempts to insert amalicious code into non validated input. The attacker tries to get the database to dump its contents.

A sample is provided below:

Var TrainCity;

Traincity – Request from (‘ TrainCity’);

Var sql = “ select * from OrderTable where TrainCity = ‘”+ TrainCity +”’”’

If the user requests the city table, the query will drop all the data in the city table. The technique used here is that the attacker will pose the query to the database about the table TrainCity. When the database responds to the query it will drop the table with the entries. This table will be dropped to the attacker, and he will have access to the information.

To avoid this, always validate all the input data that is put into the database. This ensures that all the data is from a trusted source. Another way is to apply the use of Type-Safe parameters in the SQL. The collection has a provision for checking and validating the typed parameters.

2). a) The string ^ [^s] +$ is used for matching strings that don’t have whitespaces and has one or more characters. The $ is for numerical checking. It checks for numerical inputs.

b). This will prevent SQL injection because the data input by the user is checked for validation.

3). a). After using SQL injection, the table that had the users came up. These were the names of the field being referenced. The command that was used was ‘=’. Inputting this in the name field made the database to drop the able contents. The contents are valid because they came assigned with user ID’s.

3). b). When the characters ‘=’ are input in the username text box, the results is the contents of all the usernames that can access the system. The database responds to this entry by displaying all the contents for the field entered. The result for this is the display of the contents of the username table as shown below.

The names of the users are:

id: 24

username: timmy

id: 56

username: jen

id: 0

username: wolfgang

Encryption

1. a). 999. 5893 seconds

b). 532800(6 days 4 hours)

c). 2433600(28 days 4 hours)

d). Password complexity should be limited, because the more complex they are, the higher the chance of someone forgetting. And with that complexity, trying to discover would be virtually impossible.

f). Regular Expression

^(((((25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[0-9])-(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]

{1}[0-9]{1}|[1-9]).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[0-9]))|((25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]| 0).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[0-9]))),)*)(((25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]).(25[0-5]| 2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-

2) Student ID, 98, ascii Equivalent: 57 56, Binary Equivalent 00111001 00111000

00111001 ascii 5700111000 ascii 56

00111001 cipher byte00111001 cipher byte

0000000000000001 results.

b)Students numbers are predictable because they are sequential and are assigned according to faculty. This makes it easy to predict another student’s number, to beak this cipher an algorithm is created to subtract the cipher byte from the respective ascii equivalent of the number, after they have been converted to binary.

An example Student ID number is ascii format after addition of a cipher byte 00111001 is shown below. To get the original plain text, the subtraction is done. The main trouble with the XOR decipher is it does not always decrypt accurately. Hence the plaintext might not be correct after decryption.

00001011 00001001 00001001 00001011 00001000 00001011 00001110 00001100 00001011

00111001 00111001 00111001 00111001 00111001 00111001 00111001 00111001 00111001

00110010 00110000 00110000 00110010 00110000 00110010 00110001 00110101 00110010

The plain text result is: 840436742.

This is because the logic for the XOR function is as shown in the table below.

A

B

A xor B

0

0

0

0

1

1

1

0

1

1

1

0

c)If the cipher bytes are input into the data byte by byte they will make the process more secure. The generation of the cipher bytes will be, by use of a random algorithm. The creation of random bytes makes it difficult for attackers to find the pattern. This reduces the predictability of the input data, which consequently makes it more secure.

3)In symmetric cryptography one public key is used to encrypt and decrypt the data. This means that when the data is sent, the receiver has to have the same key as the sender. Without the public key the receiver would not be able to decrypt the data. In asymmetric encryption, on the other hand, two keys are used. The public key is used to encrypt the data and a private key is used to decrypt it. This means that the sender and the receiver have different keys. In this encryption exchanging keys is not necessary.

4)Hashing involves ‘ tagging’ data with signatures that are used to identify that block of data. This leaves the data unchanged and is very useful in indexing. Encryption changes plain text data into cipher text which is unreadable by unauthorized people (Litchfield, 2003). Hashing cannot be used instead of encryption because it does not secure the data. Hashing is most commonly used in verification of files. An example is, in the storage of password, encryption is essential. This helps secure the password content from unauthorized people. However, hashing creates a hash for the password to help in verification from the database.

5)The use of third party software to manage, FileZilla password might be the best way to go. This is because, FileZilla stores its passwords in plain text and they can easily be viewed in the windows platform. The use of software developed specifically for password encryption and management would solve this problem effectively. A tool such as TrueCrypt provides encryption solutions in the windows platform. This container based encryption method, will encrypt the passwords making them more secure.

References

Litchfield, D. (2003). SQL Server Security. New York: McGraw-Hill Osborne Media.

.